UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,918	10/23/2003	Ryan Beehler	8002AC-88	6512

22150 7590 03/06/2007

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
YANG, CLARA I	
ART UNIT	PAPER NUMBER
2612	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,918	BEEHLER ET AL.	
	Examiner	Art Unit	
	Clara Yang	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-22,25-33 and 37-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-22,25-33 and 37-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892) ✓
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) ✓ Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. Examiner Matsuichiro Shimizu is no longer with the U.S. Patent and Trademark Office. Consequently, this application has been assigned to Examiner Clara Yang.

Response to Arguments

2. The indicated allowability of claims 4, 24, and 36, which have been incorporated into claims 1, 9, and 33, is withdrawn in view of the newly discovered reference(s) to Huntzicker (US 2005/0040933 A1), Rodriguez et al. (US 6,975,202), and Underdahl (US 2003/0179076 A1). Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 39 and 40 are rejected because it is incomplete due to missing elements as a result from the cancellation of claim 34. The Examiner considers claims 39 and 40 to depend on claim 33.

5. Claims 26 and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 26 recites the limitation "the security system function" in the second line of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 40 recites the limitation "the base identification" in the second line of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 5-7, 33, 37-39, and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by Huntzicker (US 2005/0040933 A1).

Referring to claims 1 and 33, as shown in Figs. 1, 4, and 6, Huntzicker's security system comprises (a) keyless entry module 10 (i.e., a wireless control device) that transmits via transmitter 34 and antenna 36 a message formed by an entry code (i.e., a unique security identification) and at least one command code (i.e., a function command) and that includes keypad 26, which is used to enter a key code (i.e., tag identification) (see Sections [0018], [0021], and [0031]). The key code is understood to correspond with the entry code since Huntzicker teaches in Fig. 6, that a valid key code must be entered at steps 110-118 before transmitter 34 will transmit the vehicle entry code at step 120 (see Section [0031]). Huntzicker further teaches that a vehicle determines if a received entry code is valid, and if the entry code is determined to be valid, the vehicle is then able to receive command codes (see Section [0032]); thus Huntzicker's security system further includes (b) an authentication control module at a vehicle that receives keyless entry module 10's command and executes the command (i.e., that grants a wireless control device's operational parameter) (see Sections [0007], [0017], and [0022]). It is understood that the entry code is a serial number since Huntzicker discloses since the entry

code is formed by a series of numbers (see Section [0016]). Because the vehicle is able to determine the validity of a received entry code and execute a received command, the vehicle must have a database storing at least one valid entry code and command that is accessible by the vehicle's authentication control module (see Sections [0021] and [0032]). Huntzicker's keyless entry module 10 comprises an authentication control module formed by keystroke detector 28 and processor 33. Per Huntzicker, processor 33 enables transmitter 34 to transmit an entry code and a command code at steps 120 and 130 respectively when processor 33 determines that the key code sequence received at step 110 is valid (see Fig. 6 and Section [0031]). Keyless entry module 10's memory 32 is accessible by processor 33 and stores a database of valid entry codes, each being a serial number, and commands (see Sections [0016], [0021], and [0031]-[0032]).

Regarding claims 5, 6, 37, and 38, as explained in the previous rejection of claims 1 and 33, Huntzicker discloses that keyless entry module 10's authentication control module comprises keystroke detector 28 connected to processor 33. Processor 33, which is a computer, must include a computer software product in order to perform the functions as shown in Fig. 6.

Regarding claims 7 and 39, as shown in Fig. 6, the authentication control module of Huntzicker's vehicle is wirelessly coupled to keyless entry module 10 at steps 120 and 130 (i.e., the time for executing keyless entry module 10's command (i.e., granting an operational parameter to the wireless control device) (see Sections [0022] and [0031]-[0032]).

Referring to claim 41, Huntzicker's security system comprises keyless entry module 10 (i.e., a control device) having (a) transmitter 34 and antenna 36 used to transmit an entry code (i.e., a unique security identification) and at least one command code (i.e., a function command) and (b) keypad 26 used to enter a key code (i.e., tag identification) (see Sections [0018], [0021], and [0031]). The key code is understood to correspond with the entry code since Huntzicker

teaches in Fig. 6, that a valid key code must be entered at steps 110-118 before transmitter 34 will transmit the vehicle entry code at step 120 (see Section [0031]). Huntzicker's keyless entry module 10 further comprises (c) an authentication control module formed by keystroke detector 28 and processor 33. As shown in Fig. 6, Huntzicker teaches that processor 33 enables transmitter 34 to transmit an entry code and a command code at steps 120 and 130 respectively when processor 33 determines that the key code sequence (which further functions as an identification code of keyless entry module 10) received at step 110 is valid (see Section [0031]). Huntzicker also discloses that keyless entry module 10 has permission to communicate with the vehicle until time delay 122 (i.e., an operational parameter provided by processor 33 of the authentication control module) has elapsed (see Fig. 6 and Sections [0031]-[0032]).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 8 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huntzicker (US 2005/0040933 A1) as applied to claims 1 and 33 above, and further in view of Sanders et al. (US 4,754255).

Regarding claims 8 and 40, Huntzicker fails to teach that a vehicle's entry code is formed by combining a key code (i.e., tag identification) and a base identification of the vehicle's database.

In an analogous art, as previously explained in the Office Action mailed on 25 September 2006, Sanders teaches forming a unique security code by combining a specific multi-digit code for an authorized operator (i.e., tag identification) and a specific multi-digit code for that vehicle (see Col. 3, lines 18-24). The multi-digit code for a vehicle is understood to also be a base identification for the vehicle's database that stores the vehicle's unique security code.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Huntzicker's security system as taught by Sanders because a vehicle's entry code that is formed by combining a key code (i.e., tag identification) and a base identification of the vehicle's database enables one keyless entry module 10 to protect all the vehicles of a multi-vehicle family while enabling a plurality of operators to use keyless entry module 10 (see Sanders, Col. 3, lines 18-24 and Huntzicker, Section [0021]).

11. Claims 9-22, 25, 26-30, 32, 42, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rodriguez et al. (US 6,975,202) in view of Dent et al. (US 7,114,178).

Referring to claim 9, Rodriguez's method comprises (a) key supplier 104 (i.e., an access control module) granting or denying wireless communication device 102 (i.e., a control device) access to electronic locking device 106 (see Fig. 5A; Col. 5, lines 46-50; and Col. 13, lines 8-17); (b) wireless communication device 102 receiving a user input via user interface 320 when key supplier 104 grants access by to a secondary key code to wireless communication device 102

(see Fig. 3; Fig. 5A, step 520; Fig. 5B, step 560; Col. 5, lines 46-54; Col. 6, lines 1-7; Col. 11, lines 25-29; and Col. 13, lines 20-21); and (c) wireless communication device 102 transmitting a message comprising the secondary key code (i.e., a security identification) to electronic locking device 106 (i.e., a security system) (see Fig. 5B, step 565; Fig. 7, step 710; Col. 6, lines 19-28; and Col. 13, lines 47-50). The secondary key code includes secondary key code portion 420, which is a base identification of a database since it is used to identify electronic locking device 106 and its table (i.e., database) of valid secondary key codes (see Fig. 4; Col. 12, lines 4-18; and Col. 14, lines 44-50). It is understood that the secondary key code is also a security system command since a valid secondary key code causes electronic locking device 106 to operate (e.g., lock or unlock) (see Fig. 7, step 740; Col. 6, lines 23-28; and Col. 13, lines 51-54); thus wireless communication device 102's message comprises a security identification and a security system command since claim 9 fails to call for the security identification and security system command to be two separate components of the message. Rodriguez's method also includes key supplier 104 generating a secondary key code that includes wireless communication device 102's identifier and key supplier 104's controller 210 using key table 230 to identify wireless communication devices used to operate an electronic locking device (see Fig. 4, device ID 430; Col. 5, lines 50-54; Col. 6, lines 36-40; and Col. 10, lines 30-36, 45-48, and 54-58); thus key supplier 104 must receive wireless communication device 102's identifier. Rodriguez, however, is silent on key supplier 104 granting or denying access based on wireless communication device 102's identifier. Rodriguez, however, does teach master key supplier 108 granting key supplier 104 access to a master key based on key supplier 104's customer identifier (i.e., an identification code) (see Col. 4, lines 34-46 and Col. 5, lines 37-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Rodriquez's method because the method of key supplier 104 determining whether or

not to allow wireless communication device 102 access (see Col. 5, lines 46-50) based on wireless communication device 102's identifier ensures that the secondary key code is transmitted to only an authorized wireless communication device 102, thereby enhancing security.

Rodriguez's method, however, further lacks wireless communication device 102 (1) receiving a tag identification and (2) determining the secondary key code based on the tag identification.

In an analogous art, Dent's method comprises (a) central controller 40 (i.e., an access control module) granting or denying wireless communication device 100 to an authorization code (see Col. 6, lines 22-41); (b) after receiving an authorization code, wireless communication device 100 deleting selected digits of the authorization code based on a personal identification number (PIN) and receiving the PIN (i.e., a tag identification) from a user via input device 102 (see Fig. 2; Col. 3, lines 58-64; and Col. 6, lines 46-52); (c) wireless communication device 100 determining the authorization code (i.e., security identification) by inserting the missing digits using the PIN, thereby determining a security identification based on the PIN (see Col. 6, lines 46-52); and (d) wireless communication device 100 transmitting the authorization code, which functions as security information and a security system command since a valid authorization code causes electronic door lock 20 to unlock (see Col. 7, lines 12-30).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Rodriquez's method as taught by Dent because the method of wireless communication device 102 (1) receiving a tag identification and (2) determining the secondary key code based on the tag identification protects the secondary key code when it is stored in an insecure memory (see Dent, Col. 6, lines 46-52), thereby enhancing security.

Regarding claim 10, Rodriguez's method, as shown in Fig. 7, further comprises electronic locking device 106 comparing the secondary key code with a stored secondary key code at step 720 (see Col. 6, lines 29-40; Col. 13, lines 48-51; and Col. 14, lines 44-50).

Regarding claim 11, Rodriguez's method, as shown in Fig. 7, further comprises electronic locking device 106 operating the lock at step 740 (i.e., executing a system command) upon determining that the secondary key code corresponds to a stored secondary key code (see Col. 6, lines 23-28 and Col. 13, lines 51-54).

Regarding claim 12, when Rodriguez's method is implemented in a rental car environment (see Col. 8, lines 51-58 and Col. 9, lines 31-44), the secondary key code is unique to the vehicle security system.

Regarding claim 13, Rodriguez's secondary key code controls a lock or unlock feature (see Fig. 7, step 740; Col. 6, lines 19-28; Col. 9, lines 31-44; and Col. 13, lines 51-54).

Regarding claim 14, Rodriguez's method also includes wireless communication device 102 transmitting (i.e., broadcasting) the secondary key code to at least two security systems, such as hotel room door lock 830, a vending machine room door lock 840, and a hotel lobby's front door lock 850 (see Col. 14, lines 16-22 and 36-38).

Regarding claim 15, Rodriguez teaches using the present invention in service industries, such as the car rental industry (see Col. 8, lines 51-58). When used in the car rental industry, Rodriguez's invention eliminates the need for a vehicle key (see Col. 9, lines 8-15 and 31-44); thus, in addition to wireless communication device 102 having the function of operating a vehicle system's electronic locking device 106 (which is understood to be a vehicle door lock), wireless communication device 102 must also have the function of starting the vehicle system in order for a customer to drive the vehicle.

Regarding claims 16 and 17, the term "permanent" is defined as "continuing or enduring without fundamental or marked change" (see the 10th edition of *Merriam-Webster's Collegiate Dictionary*). Since, Rodriguez teaches that only key supplier 104 is able to change electronic locking device 106's "frozen state" (i.e., a mode) to a normal operation (see Col. 7, lines 1-8 and 45-52), it is understood that key supplier 104 permanently defines this mode change of changing of a "frozen state" to a normal state. Rodriguez also teaches that key supplier 104 transmits key information by identifying an address or identifier of an electronic locking device and sending the key information to that address or identifier (see Col. 4, lines 59-67 and Col. 5, lines 1-5); thus key supplier 104 is a global control device.

Regarding claim 18, per Rodriguez, the only portion of a secondary key code that changes is portion 460 (see Col. 12, lines 4-56). It is understood that secondary key code portion 420, which identifies electronic locking device 106 and its table/database (as explained in the previous rejection of claim 9) remains unchanged during its lifespan as defined by activation/expiration portion 440 since electronic locking device 106 determines secondary key code portion 420's validity using activation/expiration portion 440 (see Col. 6, lines 31-36); thus secondary key code portion 420 is permanently defined in wireless communication device 102.

Regarding claim 19, Rodriguez discloses that key supplier 104 transmits a secondary key code to wireless communication device 102, thereby permitting wireless communication device 102 to transmit the secondary key code according to the secondary key code's activation/expiration portion 440 (see Fig. 4 and Col. 12, lines 35-41); thus, the secondary key code is an authentication control module message when it is transmitted from key supplier 104 to wireless communication device 102.

Regarding claim 20, as explained in the previous rejection of claims 9 and 19, the secondary key code (an authentication control module message), as shown in Fig. 4, includes

secondary key code portion 420 (i.e., a base identification), which identifies electronic locking device 106 and thus its table/database of valid secondary key code portions (see Col. 12, lines 13-18 and Col. 14, lines 44-50); hence, Rodriguez's method comprises defining the base identification of electronic locking device 106's table via the secondary key code.

Regarding claims 21 and 22, Rodriguez teaches that the secondary key code, which includes the secondary key code portion 420 (i.e., base identification) of electronic locking device 106 and its table, expires after a predetermined time interval (see Col. 5, lines 50-54; Col. 6, lines 31-35; and Col. 12, lines 35-41), as called for in claim 21, wherein the time interval is selectable in key supplier 104 (see Col. 5, lines 46-54; Col. 10, lines 30-36; Col. 12, lines 35-41; and Col. 14, lines 16-35), as called for in claim 22.

Regarding claim 25, the claim is interpreted and rejected as claim 22.

Regarding claim 26, Rodriguez's method, as shown in Fig. 6, includes key supplier 104 setting a permission for unlocking or locking (i.e., a security system function) by transmitting a secondary key code, which includes an expiration/activation time, to an authorized wireless communication device 102 at step 640 (see Fig. 6; Col. 5, lines 46-54; Col. 12, lines 35-41; and Col. 13, lines 35-42).

Regarding claim 27, Rodriguez teaches that electronic locking device 106 is only able to change from a "frozen state" to a normal state when it receives a valid master key code from key supplier 104 (see Col. 7, lines 1-8 and Col. 8, lines 33-42); thus key supplier 104 selectively sets a permission for electronic locking device 106 to change its mode from "frozen" to "normal."

Regarding claim 28, as shown in Figs. 5A and 6, Rodriguez's wireless communication device 102 transmits a secondary key code request to key supplier 104 (step 510), which receives the request (step 610) and transmits the secondary key code to wireless communication device

102 (step 630), and receives the secondary key code from key supplier 104 in step 520 (see Col. 13, lines 8-13); thus wireless communication device 102 and key supplier 104 communicate wirelessly and bi-directionally.

Regarding claim 29, as explained in the previous rejection of claim 28, Rodriguez's wireless communication device 102 and key supplier 104 communicate bi-directionally. Rodriguez discloses that wireless communication device 102 and key supplier 104 are able to communicate bi-directionally via a wired communication link, such as network 110 (see Col. 4, lines 27-33 and Col. 5, lines 21-36). Though Rodriguez is silent on connecting wireless communication device 102 to a wired communication link via a docking station, the examiner takes Official Notice that connecting a wireless communication device to a wired network via a docking station is well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made such that wireless communication device 102 and key supplier 104 communicate bi-directionally via a wireless communication link and a docking station because a docking station provides a quick and easy way to connect wireless communication device 102 to a wired network.

Regarding claim 30, Rodriguez teaches that key supplier 104 and electronic locking device 106 are in communication with one another via wireless communication links (see Col. 3, lines 36-44). In addition, key supplier 104 is able to change electronic locking device 106's various states or modes. For example, key supplier 104 changes electronic locking device 106 from an unlocked to a locked mode, from a "slow down mode" to a normal operation mode, from a "frozen mode" to a normal operation mode, etc. (see Col. 7, lines 41-52). Hence, Rodriguez's method comprises key supplier 104 wirelessly changing electronic locking device 106's mode.

Regarding claim 32, Rodriguez's customer mode provides at least a keyless entry function (see Col. 8, lines 51-65; Col. 9, lines 31-44; Col. 13, lines 51-54; and Col. 14, lines 36-38).

Referring to claim 42, Rodriguez teaches a method that controls a vehicle security system when the method is used in a rental car environment (see Col. 8, lines 51-58 and Col. 9, lines 31-44). Rodriguez's method, as shown in Fig. 6, comprises (a) key supplier 104 (i.e., an authentication control module) receiving a request for a secondary key code (i.e., a first message) that enables wireless communication device 102 to operate electronic locking device 106 (i.e., access a vehicle security system) at step 610 (see Col. 5, lines 46-48 and Col. 13, lines 10-11, 35-38, and 51-54); (b) key supplier 104 granting or denying wireless communication device 102's request (see Col. 5, lines 46-50); and (c) key supplier 104 providing a secondary key code (i.e., a second message) when access to electronic locking device 106 is granted at steps 620-640, the secondary key code, as shown in Fig. 4, including secondary key code portion 420 (i.e., a base identification of electronic locking device 106 and its table/database) and activation/expiration portion 440 (i.e., an operational parameter) (see Col. 5, lines 46-54; Col. 12, lines 13-18 and 35-41; and Col. 14, lines 44-50). Because Rodriguez's wireless communication device 102 transmits a request to key supplier 104, key supplier 104 generates a secondary key code using wireless communication device 102's identifier, and wireless communication device 102 transmits its device ID and the secondary key code to electronic locking device 106 (see Fig. 4, device ID portion 430 and Col. 12, lines 19-31), it is understood that wireless communication device 102 transmits its device ID along with a secondary key code to key supplier 104 such that key supplier 104 is able to generate a valid secondary key code. Rodriguez, however, fails to teach the method of key supplier 104 granting or denying wireless communication device 102's request based on information within a database. The examiner takes Official Notice that the method of granting or denying access to a vehicle security system based on information within

a database is well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Rodriguez's method because the method of key supplier 104 granting or denying wireless communication device 102's request based on information within a database ensures that the secondary key code is transmitted to only an authorized wireless communication device 102, thereby enhancing security.

Regarding claim 43, the limitations of the claim are previously called for in the last four lines of claim 9; thus the claim is interpreted and rejected as claim 9.

12. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rodriguez et al. (US 6,975,202) in view of Dent et al. (US 7,114,178) as applied to claim 9 above, and further in view of Underdahl (US 2003/0179076).

Regarding claim 31, though Rodriguez teaches using the present invention in service industries, such as the car rental industry (see Col. 8, lines 51-58), instead of in vehicle dealerships, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Rodriguez's invention such that it is used in a vehicle dealership since a vehicle dealership hands out keys to salespeople on a regular basis, and Rodriguez discloses that the invention may be used in industries in which the handing out of keys is performed on a regular basis (see Col. 8, lines 43-46). In addition using Rodriguez's invention in a vehicle dealership saves the cost of lost keys by making use of devices already owned by customers (see Col. 8, lines 55-65). Rodriguez and Dent, however, omit teaching a dealership mode that provides a passive arming function and a test drive function.

In an analogous art, Underdahl teaches a removable door lock control apparatus 110, as shown in Fig. 1, that allows a salesperson at a dealership to control a vehicle's door lock status and engine status (see Section [0020]). Underdahl teaches (1) unplugging removable door lock control apparatus 110's multi-car receiver 412 when the vehicle is sold (thereby placing the

vehicle in a customer mode) and (2) deactivating vehicle receiver 402 when multi-car receiver 412 is in use (thereby placing the vehicle in a dealership mode) (see Fig. 4 and Sections [0027]-[0028]). While in the dealership mode, the vehicle's control unit 314 includes a passive arming function in which timer 334 counts a predetermined amount of time from the last time that a vehicle door was unlocked and causes the doors to lock and the starter to be disabled after the expiration of the predetermined time (see Section [0026]). The vehicle further includes a test drive function in which vehicle 102's door locking system 106 unlocks a door after receiving a valid signal from transmitter 120 to allow a customer to test drive the vehicle (see Section [0021]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method and system of Rodriguez and Dent as taught by Underdahl because a vehicle security system having a dealership mode that provides a passive arming function and a test drive function provides additional security by passively arming when a salesperson forgets to lock a vehicle door after taking a customer on a test drive (see Underdahl, Section [0026]) and enables one transmitter to lock and unlock a plurality of vehicles, thereby eliminating the need to spend unnecessary overhead in organizing remote transmitters (see Underdahl, Sections [0007]-[008].

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Larson (US 5,815,557) teaches a security system, as shown in Fig. 3, comprising cellular telephone 52 (i.e., a wireless control device), clearinghouse 54 (i.e., an authentication module), and lock 56. Clearinghouse 54 transmits authorization data to cellular telephone 52 upon receiving cellular telephone 52's request to access lock 56.

⌘⌘⌘

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clara Yang whose telephone number is (571) 272-3062. The examiner can normally be reached on Tuesdays, 1:00-2:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman can be reached on (571) 272-3059. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Clara Yang

CY
28 February 2007